

August 5, 2014

Angela S. Simpson
Deputy Asst. Secretary for Communications & Information
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 4725
Attn: Privacy RFC 2014
Washington, DC 20230

Submitted via email to privacyrfc2014@ntia.doc.gov

Re: Docket No. 1405144424-4424-01

Dear Deputy Assistant Secretary Simpson:

Reed Elsevier is pleased to respond to the National Telecommunications and Information Administration's ("NTIA") request for comment regarding big data developments and how they impact the proposed Consumer Privacy Bill of Rights. In preparing our response we also considered the White House's Report, "Big Data: Seizing Opportunities, Preserving Values" ("Big Data Report") and the accompanying report released by the President's Council of Advisors on Science and Technology (PCAST), "Big Data: A Technological Perspective" ("PCAST Report").

Reed Elsevier is a world-leading provider of professional information solutions. We help scientists make new discoveries, doctors save lives, corporations build commercial relationships, insurance companies assess risk, and government and financial institutions detect fraud.

Our LexisNexis Risk Solutions business relies on big data analytics to process and analyze large volumes of data to help our customers - both businesses and government - answer questions and solve problems. LexisNexis Risk Solutions uses its unique data, cutting-edge technology, and advanced analytics to help our customers - both businesses and government - manage risk through fraud detection and prevention, identity authentication, debt collection, and intelligent risk management and modeling. LexisNexis Risk Solutions has layered specific big data capabilities on top of our longstanding experience with open source and proprietary data, including public records.

To manage, sort, link, and analyze big data, LexisNexis Risk Solutions designed the High Performance Computing Cluster (HPCC) platform. LexisNexis Risk Solutions' HPCC System technology allows our customers to process large amounts of data to make better decisions and get better results. Our HPCC System is an open source, scalable, big data processing platform that links disparate data sources together on a large scale and at high speed.

Based on our extensive experience with data analytics generally, and big data analytics specifically, we provide the following information in response to the broad questions posed in the Request for Public Comment.

A. Privacy Legislation and Big Data (Questions 1,6,7,8,12)

Despite the Big Data Report's emphasis on the unique nature of big data - specifically its volume, variety, and velocity - we believe that there is no fundamental difference for the purpose of determining legal obligations and duties between big data and conventional data sets. Reed Elsevier believes the U.S. policy framework and existing privacy laws sufficiently protect consumers in the context of big data analytics. The U.S. framework of sectoral laws has identified specific types of personal information, the misuse of which could potentially cause real harms to consumers. It focuses on regulating these types of information, leading to a flexible legal system in which harms are addressed without business being encumbered by excessive legal regulation.

For example, under the Fair Credit Reporting Act ("FCRA"), consumers are entitled to receive notice of certain adverse actions, such as denials of employment, credit, insurance, or housing, that are taken based on the use of a consumer report. The FCRA also provides consumers with the right to request a free copy of the information that a consumer reporting agency maintains about the consumer. The FCRA allows consumers to seek corrections to any data that is believed to be inaccurate or incomplete. The protections of the FCRA apply to any personal data used to generate consumer reports, including data used in big data systems.

The Gramm-Leach-Bliley Act ("GLBA") regulates financial institutions that have access to nonpublic personal information pertaining to consumers. It requires these consumers to receive an annual notice of privacy practices, and provides the consumer with the right to opt out of certain information sharing practices. The GLBA calibrates privacy protections for consumer financial information by providing consumers with transparency and choice. The protections of the GLBA apply to all covered "nonpublic personal information," including data used in big data systems.

The Health Insurance Portability Accountability Act ("HIPAA") protects sensitive personal health information created and maintained by health providers and health plans ("protected health information" or "PHI") by, among other provisions, restricting the use and disclosure of PHI for third-party activities, and providing requirements for data security. HIPAA applies to third-party business associates and their subcontractors who have access to PHI. The protections of HIPAA apply to all PHI, including data used in big data systems.

The Video Privacy Protection Act ("VPPA"), which regulates disclosure of video rental and digital viewing information, is another example of a sectoral law that protects consumer privacy. As with the other laws listed, the protections of the VPPA apply to all covered information, including data used in big data systems.

Reed Elsevier believes the U.S. policy framework and existing privacy laws sufficiently protect consumers in the context of big data analytics. If specific gaps are identified unique to big data analytics, Reed Elsevier supports the development of voluntary, enforceable industry codes of conduct to address such gaps. With the quickly evolving technology associated with big data analytics, this approach is the best way to ensure whatever standards are eventually adopted are dynamic enough to adapt with the pace of change.

B. Consumer Privacy Bill of Rights and the FIPPs (Questions 1,2,3,4,18)

The proposed Consumer Privacy Bill of Rights is patterned off of the widely used Fair Information Practices Principles (FIPPs). While the FIPPs work well in many applications, they do not work universally for every data application in every business sector. FIPPs are best suited for consumer-facing companies, where the company has an established relationship with the consumer. Many of these principles do not work well for information companies that collect

information from government agencies or third-party data sources and not directly from consumers.

The fact that information services companies do not interface directly with consumers makes many of the proposals within the Consumer Privacy Bill of Rights unworkable for these types of companies. Further, many of the FIPPs work well for information collected for marketing purposes but do not work for other applications such as fraud prevention.

Individual Control: This principle would include giving consumers a right to exercise control over personal data collection, sharing, use, and disclosure. As the White House recognized in drafting the Consumer Privacy Bill of Rights, for companies that collect personal data without direct consumer interaction, it is “impractical” to provide direct consumer choice.¹ Instead, these companies are encouraged to “go to extra lengths” to provide privacy protections, by providing a public explanation of the role they play and by inquiring into whether data suppliers provide appropriate choice to consumers. We are concerned that more burdensome requirements would severely undermine the effectiveness of our information products.

Consent requirements also do not make sense in the context of data derived from public records or information in public media sources, which make up a large volume of the data maintained by Reed Elsevier and other companies in our industry sector. These types of information – such as property records, court records, professional licenses, and the like – are required by law to be maintained by the government and are public due to the societal interest in having such information public and accessible. It would not be feasible or desirable to attempt to obtain consent in this context. A consent requirement would also conflict with constitutionally protected speech rights in both public records and media reports.

In addition, providing consumers with the ability to unilaterally withdraw consent for use of personal data would be problematic in certain applications. Because many LexisNexis Risk Solutions databases are used for law enforcement, public safety, and anti-fraud purposes, allowing consumers the ability to opt-out of having their information included in databases would significantly diminish the effectiveness of such databases and would arguably facilitate criminal behavior, allowing fraudsters and criminals to avoid detection. The right to withdraw consent would also negatively impact the ability of commercial, law enforcement, and nonprofit customers to protect crime victims and other consumers. For the same reason, an affirmative consent requirement would not work for these databases, since bad actors who do not wish to be included in these databases would simply refuse to provide affirmative consent.

Access & Correction: Requiring access and correction to databases used for fraud detection and law enforcement purposes can seriously undermine the integrity of these databases by allowing fraudsters and criminals to introduce corruption into a system. Correction as a right presumes proper intent but not infrequently correction rights are misused to alter records to conceal criminal intent, commit fraud, or gain benefits improperly. Applying these requirements across the board to all companies operating in a big data environment is not feasible and would not benefit consumers

Respect for Context: Limiting the use of data to purposes that are consistent with the relationship with the consumer at the time of collection and the context in which the data was originally disclosed could negatively impact commerce and stifle innovation and new product development. This conflict becomes most apparent where data is used for purposes not contemplated at the time of collection but where the use is consistent with sound public policy and societal interests such as the use of location information gathered from public documents

¹ Framework at 13.

and used to locate a criminal suspect. This principle would hamper big data analytics and the use of data in new ways to promote innovation and solve problems.

Accountability: The Framework supports self-assessment by companies as a means to promote accountability within an organization. Reed Elsevier strongly supports the concept of “privacy by design,” and we routinely consider privacy implications when developing new products. The purpose for which a product is developed drives decisions made about its design and content; privacy protections are a very important factor in this calculation. However, we do not support the creation of a formal self-assessment process for the private sector. Our current process for analyzing privacy concerns when creating new products is fluid and dynamic, matching our sometimes rapid timetables for product development. Imposing a rigid or prescriptive self-assessment requirement would certainly inhibit innovation across the U.S. data economy. We also oppose any requirement that self-assessments be made publicly available, potentially exposing proprietary business information and practices.

C. Data Redundancy and Data Fusion (Questions 7, 10, 17)

Reed Elsevier acknowledges that big data, while presenting enormous opportunities, also creates unique challenges, especially in the areas of data deletion and redundancy and de-identification. In particular, the PCAST Report discusses the wide distribution of data about individuals and the redundant nature of data storage as a potential challenge. Reed Elsevier recognizes this challenge. Additional data sources can increase the information available exponentially, and widely distributed data stores require more complex access control solutions. Based on our experience in handling big data responsibly, Reed Elsevier believes that technology is up to answering that challenge.

A universal requirement to delete data upon consumer request would pose potential problems while not necessarily extending privacy protections to consumers. Many data subjects share names and other identifying information. Implementing deletion requests for common names (e.g., “John Smith”) is a difficult, time-consuming process that often yields incomplete results. Moreover, allowing consumers to submit deletion requests poses the same risks of fraudsters “gaming the system” that were described above in the context of access and correction requests. Even a deletion requirement narrowed by a “reasonableness” standard could have unintended consequences. Big data systems are intertwined and used for multiple purposes, and allowing access and deletion for one or two purposes may “poison” the data for other purposes, such as fraud detection and prevention or law enforcement.

We encourage the Commerce Department to bear in mind that many of the benefits of big data are possible only due to the process of “data fusion,” i.e., merging data from different sources and seeing patterns emerge. Reed Elsevier connects the dots between billions of public records and transactions, resulting in actionable information. The results are products that have been demonstrated as critical to help fight crime; reduce fraud, waste and abuse in the tax and healthcare systems; combat identity theft and fraud; and yield many other services that help society as a whole as well as individual consumers.

We are also spearheading a number of research initiatives into differential privacy, privacy information retrieval, and homomorphic encryption. All of these technologies show promise in protecting privacy through technology applied to big data. While it is unclear which of these technologies will mature and become mainstream, we are working on a number of exciting potential technologies to enhance privacy and data security. Reed Elsevier submits that the market is best positioned to innovate in the area of privacy enhancements, and encourages the Commerce Department to allow this innovation to continue.

D. Accountability Mechanisms and Privacy Preference Profiles (Questions 13-16)

As discussed, Reed Elsevier is a strong supporter of self-assessment by companies as a means to promote accountability within an organization. However, we do not support the creation of a formal or mandatory self-assessment process for the private sector for the reasons detailed in the section on "Accountability" above.

We have similar concerns about the prospect of the government developing and imposing a framework for privacy risk management. As a sophisticated manager of data for over 40 years, we have decades of experience in assessing products and services, whether based on big data or on smaller data sets. We have built internal frameworks and processes for conducting this type of assessment while taking into account our customer base, the type of consumer data contained in a particular product or service, and the use of the product. Regulatory one-size-fits-all frameworks are not likely to be as finely tuned as what we have developed internally.

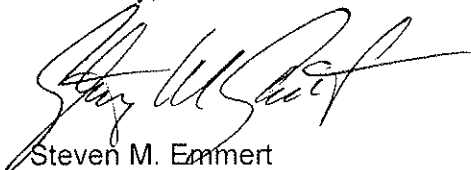
The PCAST Report's idea of "privacy preference profiles" raises a number of practical concerns, namely, how different technology providers could settle on a set of common "settings" that users could import across disparate and competing technology platforms. This type of device would have limited utility for a company such as Reed Elsevier, which does not have direct consumer facing relationships. Accordingly, Reed Elsevier encourages the Commerce Department to avoid any new requirements for the use of privacy preference profiles or other privacy-enhancing technologies, which may unintentionally disadvantage certain technologies or companies. The government should continue to take a "technology neutral" approach to privacy regulation, which enables the private market to foster the development of privacy enhancing technologies.

* * *

In summary, Reed Elsevier believes the U.S. policy framework and existing privacy laws sufficiently protect consumers in the context of big data analytics. Efforts to apply the proposed Consumer Privacy Bill of Rights in a uniform fashion across all business sectors for all applications risks hurting consumers rather than helping them. Criminals and fraudsters have sophisticated technologies and extensive data. The proposed Consumer Privacy Bill of Rights should not be implemented in a way that prevents companies like LexisNexis Risk Solutions from offering equally sophisticated tools to help government agencies and businesses protect consumers and prevent identity theft and fraud.

We appreciate the opportunity to respond to this Request for Comment and to provide our thoughts on the questions raised regarding big data analytics. If you have any questions on our comments, please contact me at (202) 857-8254.

Sincerely,



Steven M. Emmert
Senior Director, Government & Industry Affairs